Advancing Quantum Information Science

UNLOCKING *Secrets*

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY:

AN OVERVIEW

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. The NIST laboratories conduct research that advances innovation and the technology infrastructure needed by U.S. industry to continually improve products and services. NIST also promotes performance excellence among U.S. manufacturers, service companies, educational institutions, and health care providers. In addition, NIST oversees a network of local centers offering technical and business assistance to smaller manufacturers, and accelerates the development of innovative technologies for broad national benefit by co-funding R&D partnerships with the private sector.

NIST has an operating budget of about $858 million in fiscal year 2005 and operates in two locations: Gaithersburg, Md. (headquarters—234-hectare/578-acre campus) and Boulder, Colo. (84-hectare/208-acre campus). NIST employs about 3,000 scientists, engineers, technicians, and support and administrative personnel. About 1,800 NIST associates complement the staff. In addition, NIST partners with 1,400 manufacturing specialists and staff at affiliated centers around the country.

TABLE OF CONTENTS

Quantum Information Research at NIST:

Goals and Vision

America's future prosperity and security may rely in part on the exotic properties of some of the smallest particles in nature. Research on quantum information (QI) seeks to control and exploit these properties for scientific and societal benefits. This remarkable field combines physics, information science, and mathematics in an effort to design nanotechnologies that may accomplish feats considered impossible with today's technology. QI researchers are already generating "unbreakable" codes for ultra-secure encryption. They may someday build quantum computers that can solve problems in seconds that today's best supercomputers could not solve in years. QI has the potential to expand and strengthen the U.S. economy and security in the 21st century just as transistors and lasers did in the 20th century.

Quantum information is a radical departure in information technology, more fundamentally different from current technology than the digital computer is from the abacus.

William D. Phillips, NIST 1997 Nobel Prize Laureate in Physics

Nations around the world are investing heavily in QI research in recognition of the economic and security implications. A significant part of the U.S. effort is based at the National Institute of Standards and Technology (NIST), which has the largest internal QI research program of any federal agency.

NIST laboratories routinely develop the measurement and standards infrastructure needed to promote innovation in emerging fields that may transform the future. Few fields need this support as much as QI, which involves entirely new concepts of information processing as well as complex hardware for precision control of individual atoms, very small quantities of light, and electrical currents 1 billion times weaker than those in light bulbs. As the nation's measurement experts, NIST researchers long have had world-class capabilities in precision measurement and control of atoms, light, and other quantum systems. NIST, therefore, has the world-class skills and facilities needed to advance QI through technology demonstrations, development of new methods and tests for evaluating QI system components, and related scientific discoveries.

NIST first became involved in quantum information science in the early 1990s when physicist David Wineland and colleagues realized that engineering of exotic quantum states could lead to a significantly more precise atomic clock. A few years later, Wineland demonstrated the first quantum logic operation, a pioneering step toward a future quantum computer using ions (electrically charged atoms) to process information. In 1999, the NIST Physics Laboratory launched a broader Quantum Information Program, joined shortly thereafter by NIST's Information Technology Laboratory and Electronics and Electrical Engineering Laboratory.

This interdisciplinary program, featuring strong collaborations among physicists, electrical engineers, mathematicians, and computer scientists, has established NIST as one of the premier QI programs in the world. Participants include Wineland, a NIST Fellow and Presidential Rank Award winner; physicist William D. Phillips, a 1997 Nobel Prize winner in physics; mathematician Emanuel Knill, a leading QI theorist; and physicist Sae Woo Nam, winner of a Presidential Early Career Award for Scientists and Engineers. A total of nine technical divisions within three different laboratories at NIST's Gaithersburg and Boulder campuses are involved.

NIST's work in ion-trap quantum computing is widely recognized as one of the most advanced QI efforts in the world. Scientists building the NIST quantum communications testbed

Physicists Dietrich Leibfried and David Wineland lead NIST's quantum computing research using trapped ions.

set a record in 2004 for the fastest system for distributing quantum cryptographic "keys," codes for encrypting messages that, due to the peculiarities of quantum physics, cannot be intercepted without detection. Other NIST research with single photon sources and detectors, and computing with neutral atoms and "artificial atoms" are also among the leading efforts worldwide. For instance, prospects for practical quantum communications have been improved by NIST's recent demonstration of a device that detects single photons with 88 percent efficiency, a QI record.

There is strong synergy between NIST's core mission work on measurement and standards and the QI research program. For instance, NIST scientists gained much of their expertise in quantum systems from decades of work developing atomic clocks. NIST's ultra-precise atomic fountain clock—the world's most accurate device for measuring time—is based on the precise manipulation and measurement of two quantum energy levels in the cesium atom. This clock would neither gain nor lose one second in 60 million years (as of March 2005), an accuracy level that is continually being improved. NIST quantum computing research is producing new techniques that may lead to even more accurate atomic clocks in the future.

Ultimately, NIST measurements, tests, and technologies for quantum information science are helping U.S. industry develop new information technologies in an effort to ensure U.S. technological leadership and strengthen national security. The United States may have the lead in this field for now—based in part on NIST's contributions—but competition from Europe, Japan, Australia, and developing countries such as China is strong and growing.

WHAT GOOD IS QUANTUM INFORMATION?

Quantum information is the latest science behind secret codes and code breaking, essential tools for commerce and security.

Secret codes and code breaking have played dramatic roles in world history. The Nazis had a critical advantage early in World War II, for instance, thanks to the secrecy of their military communications, encrypted by the legendary Enigma machine. But eventually, Nazi messages were being deciphered routinely by mathematicians and other cryptanalysts, with the help of sailors and secret agents. Code-breaking technologies and ingenuity gave the Allies a significant advantage.

More recently, encryption has been described as a leading technological advance of the last millennium. NIST's current Advanced Encryption Standard, for example, ensures the security of billions of dollars in electronic transactions every day.

Quantum systems may provide the new "locks and keys" for information. Quantum computers, if they can be built, could break today's best public-key encryption systems, used to protect commercial communications. At the same time, quantum communications systems, if well designed, provide a new approach to "unbreakable" encryption to keep messages secret. Quantum cryptography systems are already being commercialized, and the market is predicted to reach hundreds of millions of dollars within the next few years.

Quantum computers also could have other applications. They potentially could be used to optimize complex systems such as airline schedules, accelerate database searching, and develop novel products such as fraud-proof digital signatures. Or they might be used to simulate other quantum systems, such as complex biological systems, for the purpose of designing new drugs. The history of science suggests that important applications will arise that cannot be imagined today; in 1947 when the transistor was invented, no one envisioned the $600 billion U.S. electronics and related industries it would create.

Research on quantum information is also likely to have important spin-offs in measurement science. The ability to precisely engineer quantum states may lead to the development of improved atomic clocks and advanced navigation instruments. The work also will support advances in nanotechnology, a field that has become a national priority.

Success in these applications is not assured. Many technical challenges need to be overcome before the full potential of quantum information systems can be demonstrated and exploited. The research described in this brochure is only the beginning of this work.

What Is Quantum Information?

Quantum information systems can transcend the physical limits of today's computing and communications technologies. Transistors and other electronic components have been shrinking in size for many years. When they get close to the size of single atoms, they will be miniaturized out of a job. Atomic-sized circuits cannot be made to function in conventional ways, in part because of the inability to dissipate heat and in part because they do not behave like their larger counterparts. Thus, at the smallest scales, scientists need to take advantage of a different set of design rules.

Entanglement is a much stronger relationship than we typically see in the macro world, even between identical twins.

Carl Williams, chief, NIST Atomic Physics Division

These are the rules of quantum mechanics, nature's instruction book for the smallest particles of matter and energy. First developed by Albert Einstein, Niels Bohr, and other physicists during the early years of the 20th century, quantum mechanics is the most fundamental and successful set of principles and equations known at this time for predicting the behavior of particles such as atoms and electrons, and electromagnetic radiation such as light and radio waves. Quantum mechanics plays an important role in many modern technologies. It describes a world where energy is measured and exchanged only in discrete, measurable units, or quanta. It is also a world of counterintuitive "weirdness" where objects behave in exotic ways—existing in two places at once, for example—that have no precedent in everyday, macroscopic life.

Today's digital information systems represent 1s and 0s using tiny electrical switches, which are either on or off, or the orientation of a magnet up or down, or the presence or absence of light. The information in such a device or light signal is called a bit. In quantum information processing, various quantum mechanical states of individual particles or systems are used as quantum bits (qubits). For instance, ions (charged atoms) may have different "spin" states that can represent 0 and 1. Spin can be thought of as the direction of a little compass needle inside the ion, with north and south poles. "Spin up," corresponding to 0, has a greater energy than "spin down," corresponding to 1. Similarly, single photons (the smallest quantities of light) can be transmitted in different orientations, or directions of their electric field, to represent 0 and 1.

Amazingly, qubits can be a combination of both 0 and 1 at the same time, a property called *superposition*. Qubits also can be correlated with each other, even at a distance—a property called *entanglement*. It is these unusual properties that give quantum information its power.

SUPERPOSITION

Qubits can process far more information than today's digital bits because they can exist in a "superposition" of two quantum states that, at a given moment, has some combination of both 1 and 0 at the same time.

A qubit can be in any one of an infinite number of possible superposition states at a given time, as long as it is not being measured. In the graphic below, this is represented as any one of many possible ion spin directions in between up and down (right image). Superposition states always collapse to 0 (left image) or 1 (middle image) when the qubit is measured. The fate of a superposition state in which the spin is depicted

Ions can be spin up (left image) to represent 0 or spin down (middle image) to represent 1. A superposition of both states at once can be represented graphically as any one of many possible spin directions in between up and down (right image).

Counting
WITH QUBITS

↑ = spin up

↓ = spin down

	binary code	number
↑↑↑	= 000	= 0
↑↑↓	= 001	= 1
↑↓↑	= 010	= 2
↑↓↓	= 011	= 3
↓↑↑	= 100	= 4
↓↑↓	= 101	= 5
↓↓↑	= 110	= 6
↓↓↓	= 111	= 7

as horizontal is, when measured, spin up 50 percent of the time and spin down 50 percent of the time.

To understand why superpositions are so important, compare the processing power of a hypothetical three-qubit quantum computer to a conventional three-bit computer. Three conventional bits can store just one of eight numbers from 0 to 7 in binary code (see above).

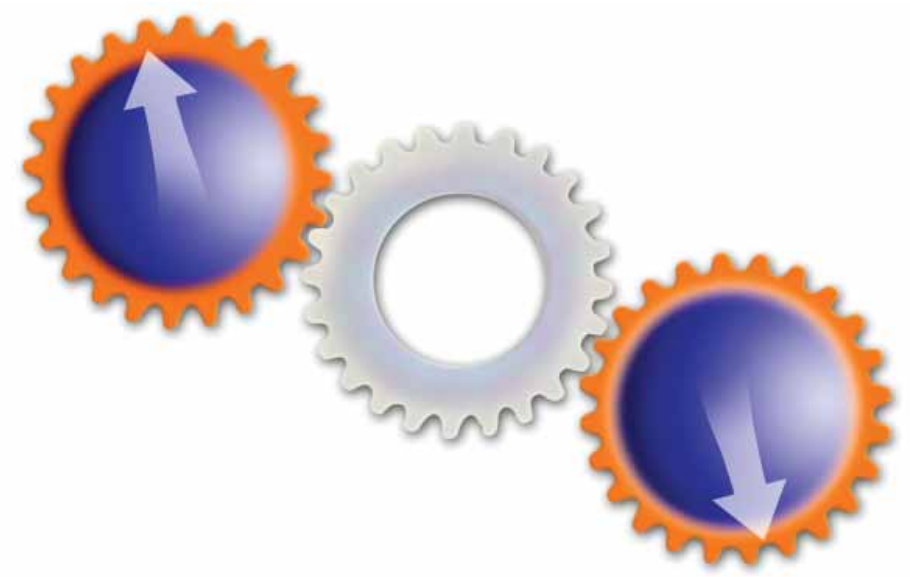
Three qubits can store all eight (2^3) such numbers at once thanks to the "magic" of superposition—an exponential increase. This also means that, effectively, eight calculations could be carried out at virtually the same time using just three qubits. This is a built-in capability for parallel processing, using far fewer bits than would be needed for simultaneous computations in today's classical computers. With a few hundred qubits, a quantum computer could have far more power than even a network of the world's best supercomputers working together.

ENTANGLEMENT

Conventional computers use programmed logic operations and specialized circuits to perform calculations and solve problems. These are the software and hardware equivalents of "if/then" statements. For instance, a particular logic operation that combines two bits to get one result might work as follows: If either bit has the value 0, then the output is 1; otherwise, the output is 0.

Through a quantum version of a logic operation on two qubits, the qubits become entangled. If one of these qubits is measured, its fate is correlated with that of the other qubit, even if the two are widely separated. Einstein called entanglement "spooky action at a distance." Entanglement sounds supernatural but in fact can occur spontaneously when two atoms, for example, are in close proximity. The atoms' properties and behavior become linked in predictable ways, and may remain so even if the atoms are physically moved apart. Entangled atoms can be compared to dance partners who do not touch each other but somehow synchronize their movements. While real dancers may do this through subtle communication, the qubit partners somehow do this without communicating, even though the dance steps may differ each time. This is what makes it "spooky."

Entanglement needs to be precisely controlled to be useful in information processing, a difficult task. Scientists have learned how to control entanglement of small numbers of atoms and photons. The effect can be visualized as a set of gears moving two atoms in tandem (see image below). There are no real gears in quantum entanglement, however; the atoms just "know" what to do on their own. Controlled entanglement is a unique quantum resource that offers, for example, a way of transmitting data or performing controlled interactions on distant quantum bits, as long as a classical communications channel is also available.



Entanglement creates correlations in properties and behavior without any physical contact. The effect can be visualized as a set of gears moving two atoms in tandem.

Quantum Computing

Quantum computing offers the possibility of parallel processing on a grand scale. Unlike switches in today's computer chips, which are either on or off, qubits can be in superpositions of both on and off at the same time, and entangled so that their properties are correlated even if the qubits are moved apart. Properties like this could enable a quantum computer to solve certain problems in an exponentially shorter time than today's computers. Researchers often point out that, for specific classes of problems, a quantum computer with 300 qubits potentially has more processing power than a classical computer containing as many bits as there are particles in the universe.

Whether or not quantum computing becomes practical, this work is producing new ways to design, control, and measure the quantum world of electrical systems.

Raymond Simmonds, NIST physicist

NIST GOALS

Demonstrate a simple quantum processor of about 10 qubits

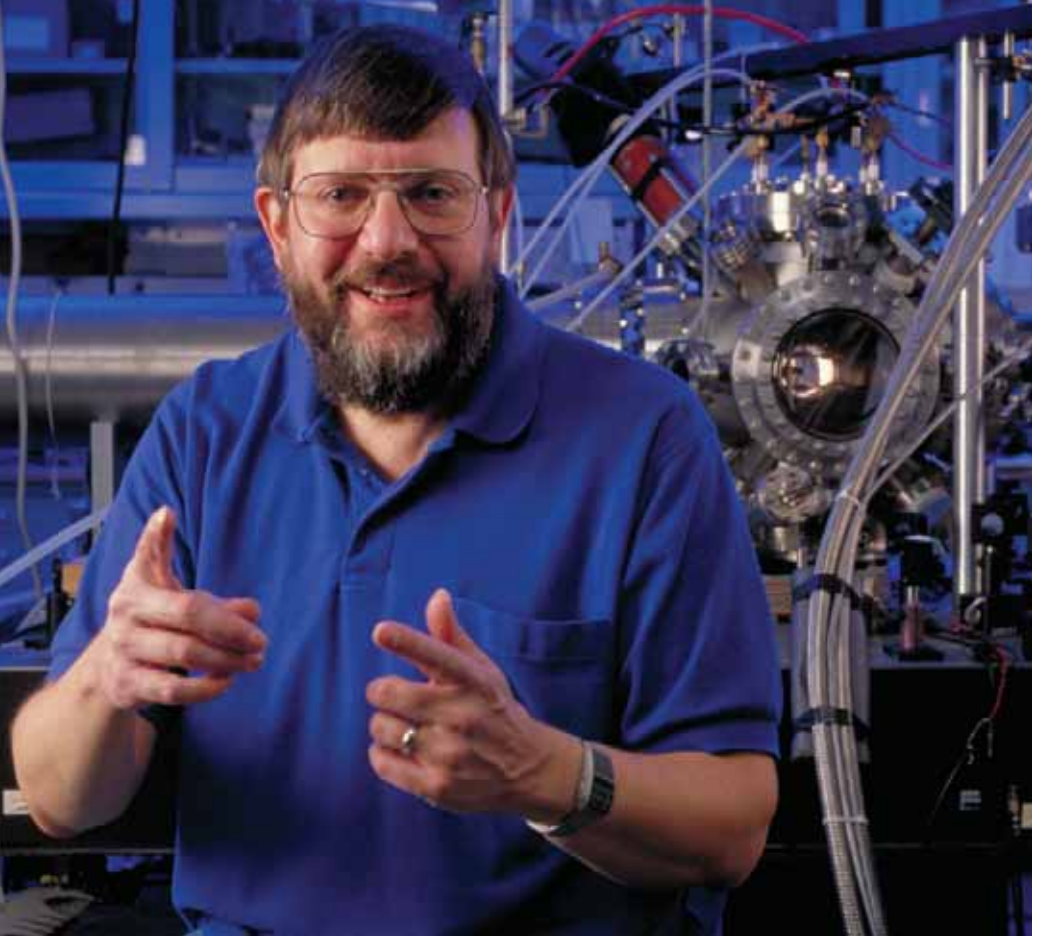
Perform repetitive quantum error correction on 3 or more qubits

Demonstrate a quantum repeater for long-distance quantum communication

Use quantum logic to improve the performance of frequency standards

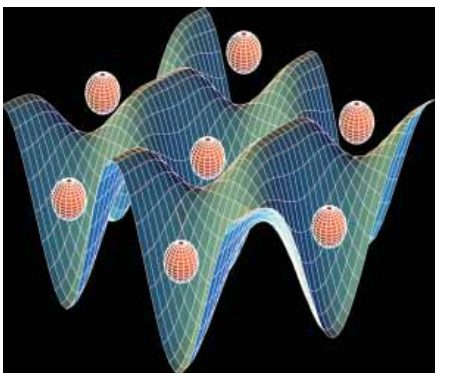
For instance, the security of today's most common cryptographic systems relies on the difficulty of "factoring" large numbers—figuring out which smaller prime numbers, when multiplied together, equal the large number. Today's computers cannot factor large numbers in reasonable amounts of time. A network of classical computers (with trillions of bits and trillions of operations per second) would need to operate for years to factor a 200-digit number, whereas a relatively small quantum computer consisting of 100,000 qubits might do it in just a few minutes or less.

Applications may extend far beyond breaking today's best encryption codes. Many physicists, computer scientists, and mathematicians are excited about quantum computing because they believe that new insights needed to build such a machine will lead to important discoveries about information processing and, more generally, about the universe by solving problems that cannot even be attempted today. New tools developed for quantum information science may help unlock secrets of nature, using quantum mechanics to explain how literally everything works.



Nobel laureate William Phillips leads NIST research on the use of neutral atoms as qubits (*left*).

The illustration below shows how neutral atom qubits can be trapped in an optical lattice made of intersecting laser beams.



But harnessing all this potential is extremely difficult. Researchers need to find ways of controlling and measuring delicate quantum states while minimizing electronic "noise" and ensuing computational errors. The challenge becomes greater as the number of qubits grows. In addition, to make full use of a quantum computer, scientists must design new software programs that can take advantage of the unusual quantum properties. These software packages must be far more efficient than conventional computer programs.

Many basic components and tools of quantum computing already have been demonstrated. These experiments generally require a roomful of equipment. Several ions (charged atoms) in a trap, for example, need to be kept in a housing 0.03 cubic meters (1 cubic foot) in size and manipulated with a laser system spread over two large optical tables, controlled by huge racks of electronics. Someday, scientists might find a way to squeeze as many as 1 billion neutral atom qubits into a processor smaller than a sugar cube. But it is expected to take years, perhaps decades, to build a useful quantum computer, regardless of the design.

NIST is pursuing three separate approaches to quantum processing: trapped ions, neutral atoms, and "artificial atoms" made of superconducting electrical circuits. While other technical approaches are being pursued at other institutions, NIST researchers believe these three types of qubits provide the best near-term possibilities for breakthroughs while also having potential applications to other NIST mission activities. Because this work is very long term, these are largely independent projects exploring potential quantum computing technologies. However, knowledge of complex quantum systems obtained from one or more of these projects may contribute insights and help create new paradigms for the others.

ION QUBITS

One of the world's best-known quantum computing efforts is the work with ion traps by the NIST Boulder, Colo., group led by David Wineland. This group uses ultraviolet lasers to manipulate the quantum states of beryllium ions in electromagnetic traps, and uses tiny electrodes to move the ions within a trap.

This work originated in the 1980s, with research on frequency standards using trapped ions. The technology was promising but there was a lot of "noise" or interference in the signal. Wineland and his collaborators developed a concept for reducing the noise below the usual limit through what was then called *spin squeezing*, a process now more generally referred to as quantum entanglement.

Also in the 1980s, prominent scientists elsewhere (Paul Benioff at Argonne National Laboratory, Richard Feynman at California Institute of Technology, and

BEAM ME UP, EINSTEIN!
NIST Demonstrates Teleportation

NIST physicists were the first, along with a team in Austria, to "teleport" data from one atom to another. Teleportation could enhance the speed and efficiency of quantum computing by transferring data between distant qubits, or it could be a crucial step in detecting and correcting minor errors.

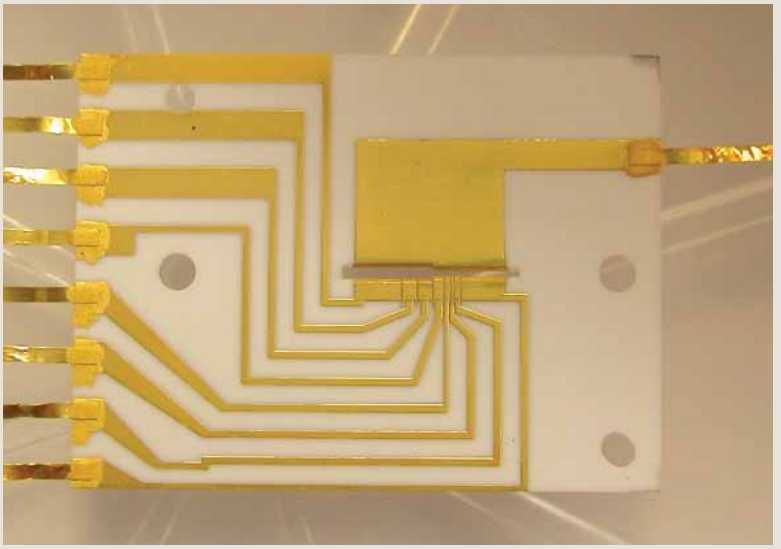
Unlike the "beaming" of people and objects between distant locations popularized in the *Star Trek* science fiction series, quantum teleportation describes the transfer of key properties of one atom to another atom without direct physical contact between them.

This may sound like magic. But teleportation merely exploits exotic features of quantum mechanics called superposition and entanglement (see "What is Quantum Information" on page 3).

Teleportation transfers the quantum properties of one atom to another atom. This includes the atom's "spin" (which may be anywhere between spin up and spin down, representing 0 or 1 or both at the same time) and its "phase" (orientation to the left or right of a vertical plane). Scientists cannot simply measure and copy the spin and phase values, because single measurements reveal only a very small amount of information and destroy delicate quantum states.

Teleportation has been compared to faxing in that it reconstructs a quantum state indirectly. But, unlike faxing, it also destroys the original. The spin and phase values are teleported in two parts. The first part is transferred by entanglement; the other part is transferred by "corrections" using more conventional tools.

The NIST procedure teleports the quantum state of one beryllium ion to another ion. Three ions are required. First, two of the ions, say ions 1 and 3, are entangled and then placed in separate locations labeled A and B, respectively. Suppose ion 2 is also located at position A and is in a quantum state to be teleported to ion 3 in position B. Now ions 1 and 2 are manipulated so they become entangled, which indirectly shares information between ions 2 and 3. Then ions 1 and 2 are measured. The result will be one of four possible combinations of 0 and 1 (00, 01, 10, and 11). The result indicates the assumed state of ion 3, and which of four possible corrections need to be applied to ion 3 to complete the teleportation. The options are: (1) do nothing, (2) reverse the spin, (3) reverse the phase, or (4) reverse both spin and phase.



Teleportation takes place between two locations inside an ion trap made of gold electrodes deposited onto alumina. The trap area is the horizontal opening near the center of the image.

later David Deutsch at Oxford University) developed the idea of quantum logic, suggesting that quantum systems could perform some computations more efficiently than classical computers. In 1994, Peter Shor of Bell Labs made a significant advance when he developed a quantum algorithm that could factor large numbers efficiently. In 1995, Ignacio Cirac and Peter Zoller at the University of Innsbruck, stimulated by discussions presented by Artur Ekert of Oxford University, made the critical link between the ion-trap research at NIST and the idea of quantum logic.

Within a few months the NIST group demonstrated the first quantum logic gate. This has been followed by numerous other accomplishments in quantum information science, many of them "firsts." The group was the first to demonstrate the entanglement of four qubits, the teleportation of atomic qubit states (see sidebars above and on page 8), and the use of quantum logic to improve measurements. The group has demonstrated all of the building blocks for a quantum computer based on ion traps. A significant advantage of ion qubits is the potential for linking together a large number of small, interconnected traps to make a computer of a practical size.

It's hard to quickly move qubits in order to share or process information. Teleportation could allow much faster information transmission and logic operations.

David Wineland, NIST Fellow

NEUTRAL ATOM QUBITS

In 2000, William D. Phillips started NIST's second effort in quantum computing, this time using neutral atoms as qubits. This effort builds on the laser cooling work for which Phillips shared the 1997 Nobel Prize in Physics and the creation of Bose-Einstein condensates (BECs) at JILA, a joint institute of NIST and the University of Colorado (CU) at Boulder. The work on BECs led to the 2001 Nobel Prize in Physics for Eric Cornell of NIST and Carl Wieman of CU.

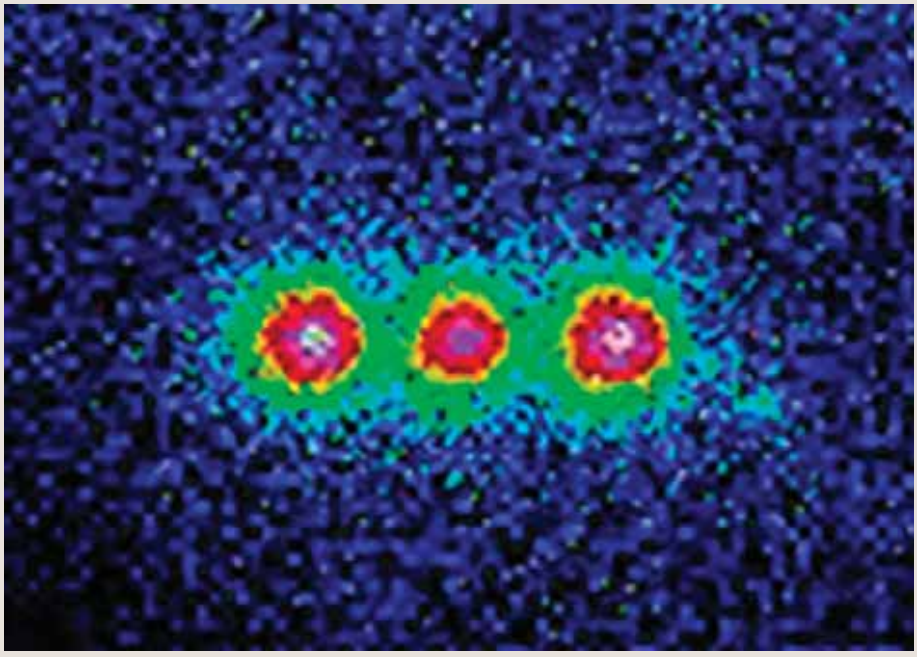
Phillips and his group at NIST's Gaithersburg, Md., campus are working with large numbers of rubidium atoms confined in optical lattices, which are arrays of egg-carton-shaped traps created by intersecting laser beams (see graphic on page 6). Scientists use the lasers to manipulate the atoms' internal energy levels. Neutral atoms are attractive as qubits because their weak interaction with the environment can reduce computing errors, but this also can reduce the speed of logic operations. The atom/lattice system may prove to be a powerful tool in physics research, because it can efficiently emulate solid-state systems that are too difficult to simulate with conventional computers.

The NIST group has taken steps toward controlling atom qubits by loading every third site of an optical lattice with atoms from a BEC, a state of matter in which millions of atoms are condensed into a single macroscopic quantum state. The group also has performed the unusual feat of making atoms that ordinarily tend to bunch together, as in BECs, behave like another class of atoms that avoid each other. This behavior allows the researchers to put about 100,000 qubits, each in a unique location, into the 0 state all at once.

ENGINEERING SECRETS: *How to Entangle Ions*

The teleportation of atomic states—an automated process requiring 4 milliseconds in current experiments—is an outcome of many NIST achievements in ion-trapping hardware engineering. A trapped beryllium ion is about 10 nanometers (billionths of meter) in diameter. NIST physicists designed an electromagnetic apparatus smaller than a penny that traps a number of ions within an area smaller than a grain of rice. Tiny electrodes are used to move ions between zones so they can be manipulated, either individually or in sets of two or three, with ultraviolet laser beams. Environmental conditions such as electronic "noise" are precisely controlled to avoid unintended atom motions.

NIST physicists developed a procedure for entangling ions in a controllable way. Two laser beams are positioned at right angles to apply an oscillating force to a pair of ions. The lasers are tuned so the difference between their frequencies is very close to the frequency of the ions' natural vibrational motion. If both ions are in the same spin state, the lasers have no effect. If the ions are in different spin states, they feel an opposing laser force that causes the ions to stretch apart. If the ions are in superpositions, the stretching motion reflects a condition of being excited and not excited at the same time. This coupling of spin states with stretching motions has the effect of entangling the two ions in a controlled way.



Three beryllium ions are entangled in pairs in NIST teleportation experiments. This colorized image shows the fluorescence from three trapped ions illuminated with an ultraviolet laser beam.

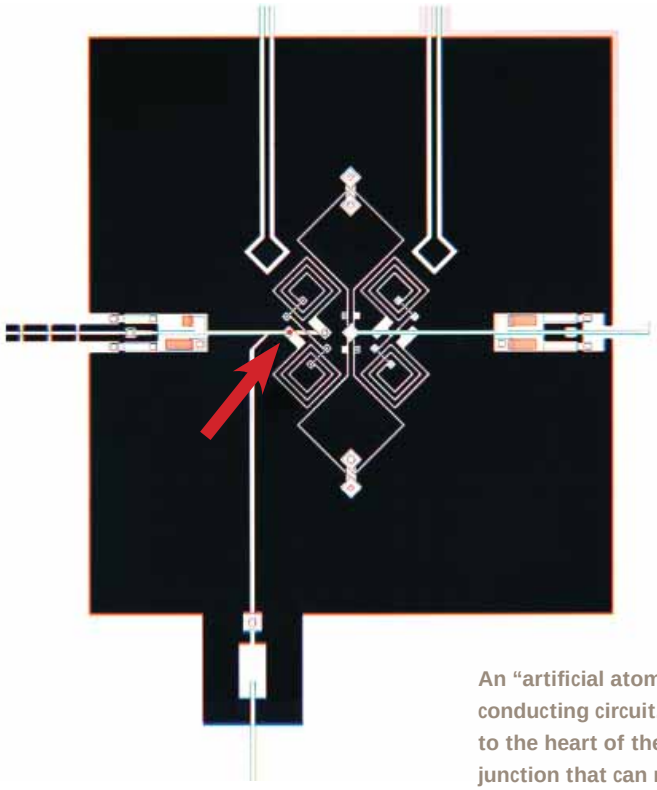
Physicist Raymond Simmonds leads the NIST research on superconducting qubits.

SUPERCONDUCTING QUBITS

In 2002, NIST began a third effort in quantum computing using "artificial atoms" as qubits. This effort, led by physicist Raymond Simmonds in NIST's Boulder laboratories, uses superconducting Josephson junctions. These solid-state devices consist of two superconducting pieces of metal separated by a thin insulating region, with the special property of being able to support a "super flow" of current. Two different energy levels of the superconducting circuits are used as the qubit states, just as spin up and spin down are used in an atom.

Superconducting qubits could perform logic operations much faster than ions or atoms. In addition, because Josephson junctions have been used in measurement science for decades, these qubits could be easily manufactured, easily connected to each other and to integrated circuits, and mass producible using microfabrication techniques. This technology enables easy communication between quantum systems but makes it difficult to isolate the whole system from various sources of electronic "noise." As a result, significant improvements are needed in system design and materials processing.

This group has made a number of impressive demonstrations, including orchestrating the behavior of two coupled qubits to witness their entanglement over time. This is a tremendous step forward. It opens the door to performing simple logic operations between two superconducting qubits, a necessary building block for the construction of a full-scale superconducting quantum computer.



An "artificial atom" is made with a superconducting circuit. The red arrow points to the heart of the qubit—the Josephson junction that can represent a 0, 1, or both values at once.

Quantum Communications

Security services are critical to modern telecommunications. For instance, they help ensure that the message received is the one sent, and that secrets remain secret. The most sensitive information, such as bank transfers, can be encrypted very effectively. But some widely used encryption systems could be defeated by quantum computers. And even if information is encrypted, an eavesdropper can still tap into a conventional communications channel and listen to or copy a transmission without being detected.

There are no commonly accepted standards for measuring and certifying the performance of quantum cryptographic systems. NIST is in a unique position to provide technical expertise in this field and to lead the development of an appropriate standards infrastructure.

Charles Clark, chief, NIST Electron and Optical Physics Division

NIST GOALS

Develop and operate a testbed for quantum communications components and protocols

Demonstrate quantum key distribution (QKD) at speeds fast enough for practical use

Develop light sources that produce single photons on demand

Develop reliable single-photon detectors

Work with industry and academia to build a standards framework for QKD

Quantum mechanics offers the potential for ultra-secure communications because a measurement of an unknown quantum system changes its state. As a consequence, accurate copying is impossible, and the changes caused by eavesdropping can be detected. Whereas today's fiber-optic communication systems require bits made of tens of thousands of photons, quantum communication uses single photons to transmit 1s and 0s. This is the future of encryption technology.

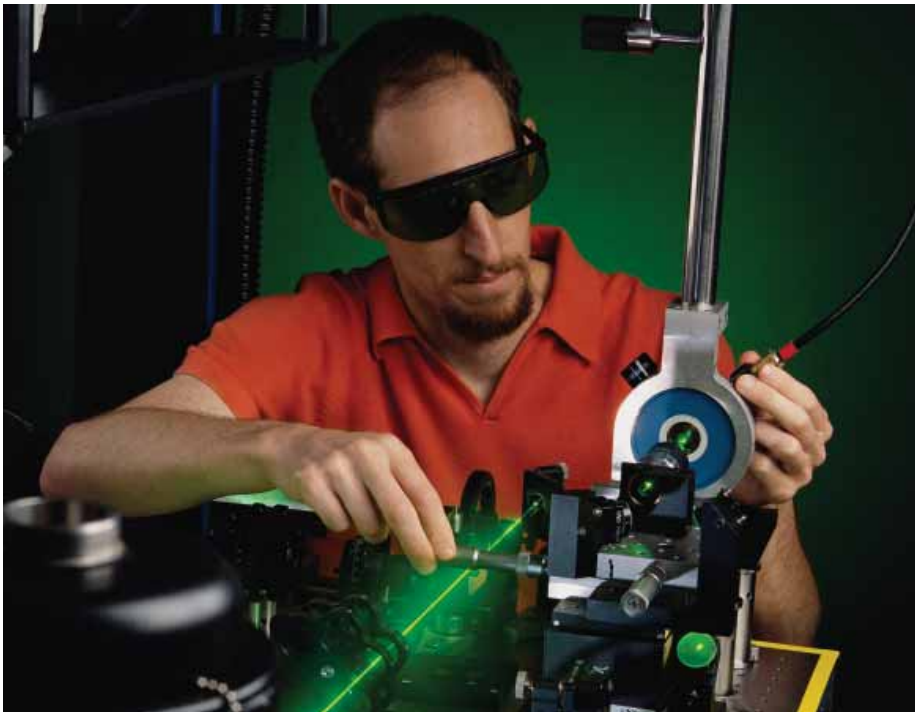
Very weak laser pulses are created so that a single pulse rarely has more than one photon. The photons are oriented for transmission through the air or cables, detected with special receivers, and interpreted by custom electronics and software. The idea is straightforward but the implementation is markedly less so. In particular, it is difficult to build fast, reliable, long-distance quantum channels, process the information generated at high speeds, and connect quantum links to networks.

One mode of quantum communications that is moving from the laboratory to early commercial production is quantum key distribution (QKD). (See "Making a Quantum Key" on page 12.) QKD provides a secure method for distributing a secret key between two parties, who then can use the key to encrypt and decrypt a message. Secure distribution of such keys remains a difficult challenge.

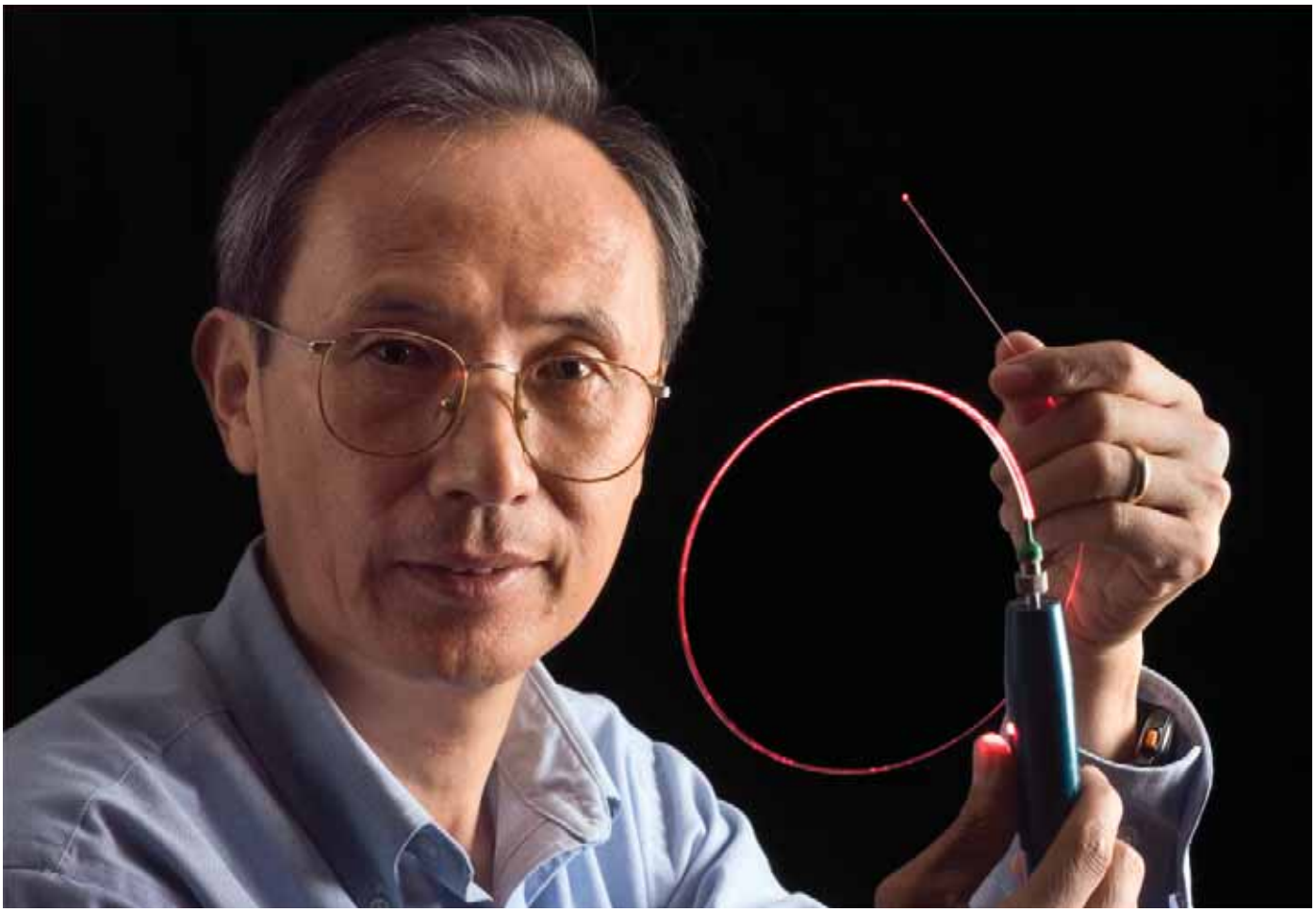
NIST is working to overcome these challenges by addressing hardware engineering issues, such as how to produce and detect single photons rapidly and reliably, and development of tools for faster and better processing of information. In addition, NIST is providing the metrology infrastructure for the development of quantum communications technologies as commodities on an industrial scale: the basic measurements needed to certify the quantum performance of components and integrated systems and to assure their conformance with standards.

QUANTUM COMMUNICATIONS TESTBED

NIST has built an open system for research, testing, calibrations, and technology development in a real-world, gigabit Ethernet telecommunications environment. At the testbed, infrared lasers generate single photons that are sent and received by telescopes over a



Engineer Richard Mirin is developing single-photon sources based on quantum dots (*above*).



Physicist Xiao Tang leads a team using optical fiber to design NIST's second quantum key distribution system (*below*).

MAKING A QUANTUM "KEY"

Quantum cryptography allows two parties, known as Alice and Bob, to exchange information in a manner that is, in principle, secure. By using single photons to encode information, Alice and Bob can detect attempts at eavesdropping.

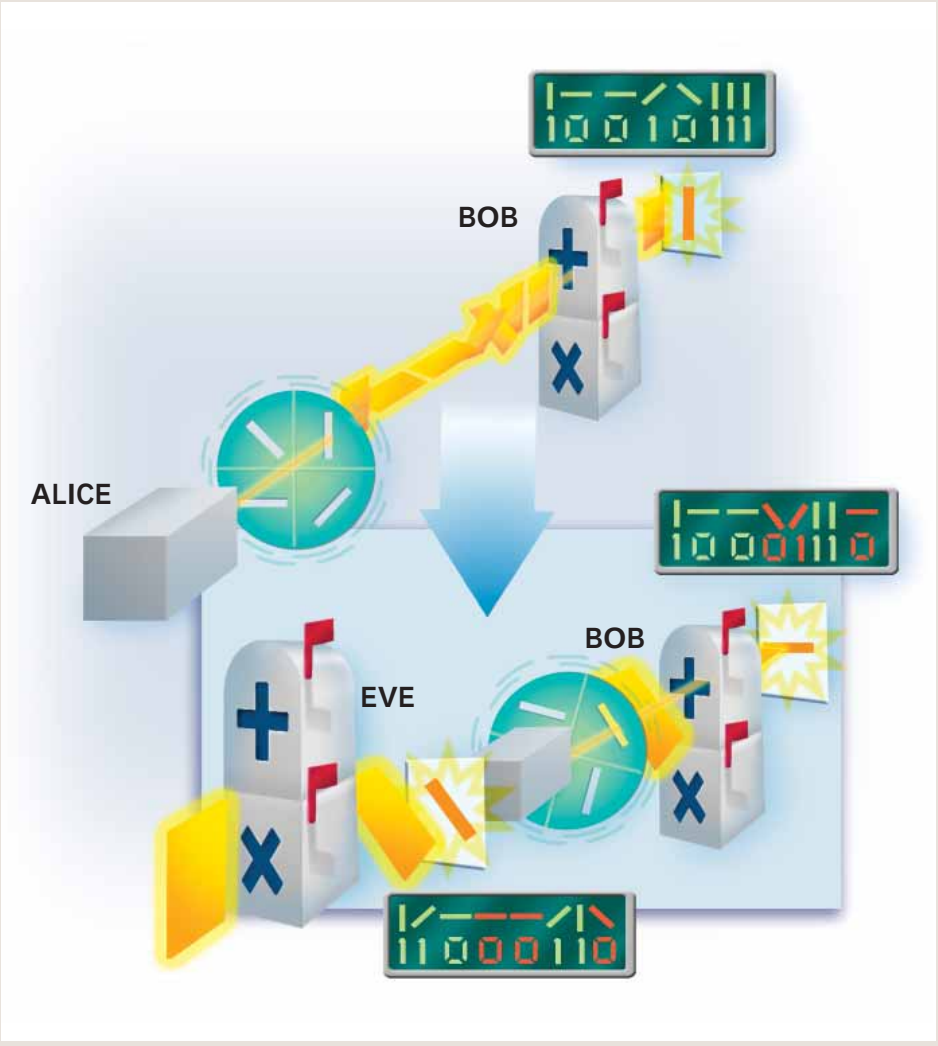
NIST is demonstrating prototype technologies for practical distribution of secret quantum keys, which are used to encrypt and decrypt messages. The NIST system sends and receives photons in four different orientations to represent the values 1 and 0. Each photon is sent in one of two modes, either vertical/horizontal orientations of the electric field, or plus 45 degrees/minus 45 degrees orientations. Within each mode, one orientation represents 0, and the other represents 1.

To visualize how this works, imagine that each photon is a tiny envelope moving perpendicular to the ground (vertical=1), parallel to the ground (horizontal=0), tilted at 45 degrees to the right (plus 45 degrees =1) or tilted 45 degrees to the left (minus 45 degrees=0). Each photon fits best through one of two types of detectors, or "mailboxes."

Alice randomly chooses both a mode and an orientation for each photon. Bob randomly chooses between the two modes when he tries to detect a photon. This can be visualized as choosing a mailbox slot that accepts only envelopes flying in certain orientations. If he chooses the same mode that Alice used for a particular photon, then Bob always measures the correct orientation, and hence, its bit value. But if he chooses a different mailbox, then he may get the wrong bit value for that photon.

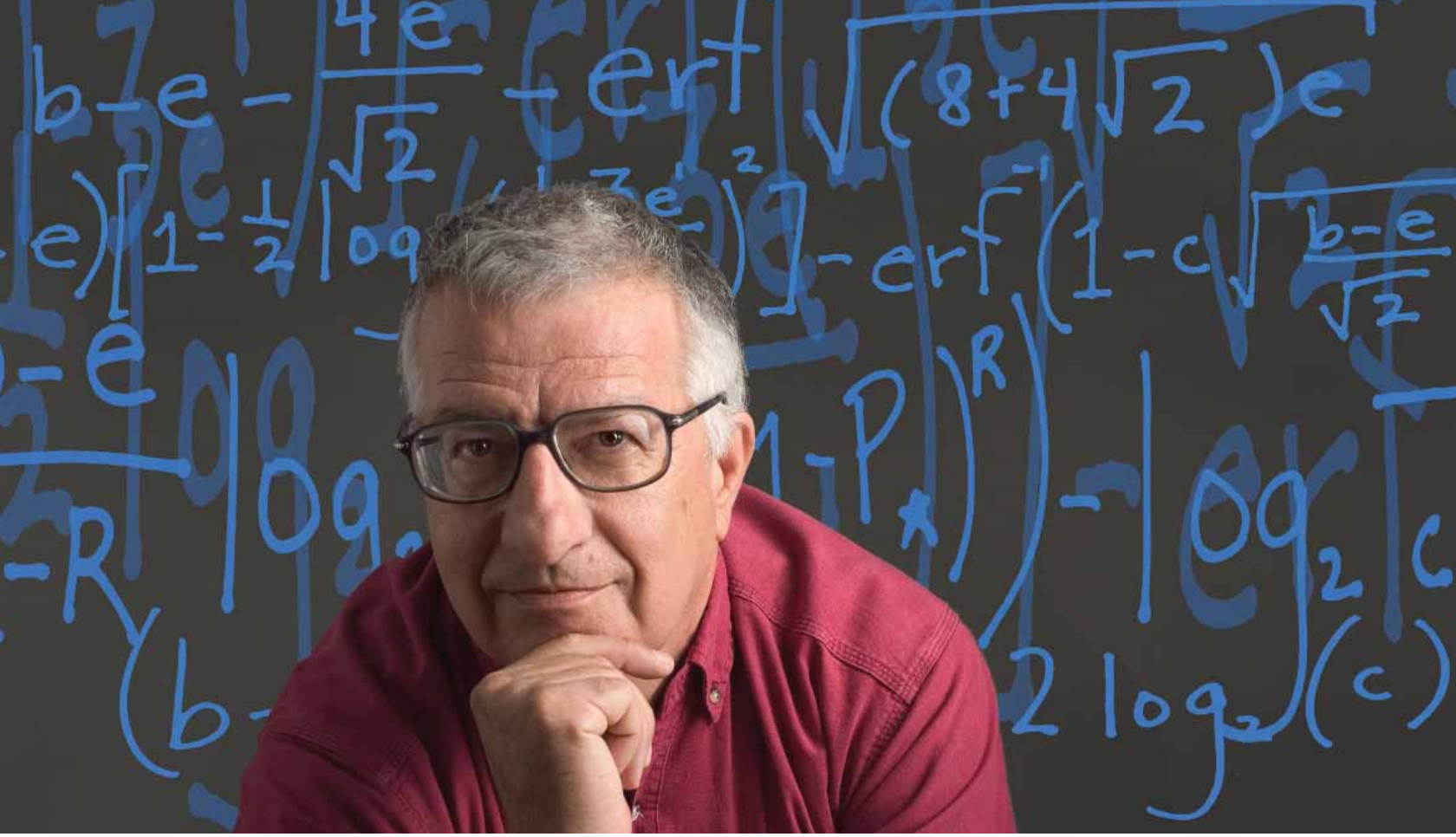
To make a shared "key" from a stream of photons, Alice uses a conventional communications channel to tell Bob which mode she used for each photon (without revealing its bit value). Bob tells Alice which photons he measured using the correct mailbox (but again, not sharing their values). Then they both discard the other bits, the ones Bob measured with the wrong mailbox. The correct measurements constitute the secret key that Alice and Bob now share.

If someone, generally referred to as Eve, tries to eavesdrop on the transmission of the stream of photons, she will not be able to "read" it without altering it. When she measures a photon, it is converted to electrical energy and destroyed. This photon will not reach Bob and will not contribute to the key. Eve may send a replacement photon, but, because she may have used the wrong mailbox to intercept the original photon, she may be wrong about the bit value. Thus, for photons detected with the wrong mailbox mode, Eve may introduce errors into the key constructed by Alice and Bob. When Alice and Bob detect an unusual number of errors they will be alerted to Eve's presence.



The illustration shows an example. If Alice sends a photon in the vertical orientation, and Bob chooses the correct mode or mailbox (the + mode), then he will always measure the photon correctly and get the correct bit value of 1. (See top of illustration.) On the other hand, if he chooses the wrong mailbox (the X mode), then he might get the wrong bit value when he measures the photon. In this case, Alice and Bob will find out later that they used different modes, and discard that bit value in making their shared key.

If Eve intercepts and resends the photons, errors occur in the data that alert Alice and Bob to the eavesdropping. In the inset picture, Eve tries to receive a vertical photon in the wrong mode and measures it incorrectly as a -45 degree photon. Eve then sends a -45 degree photon to Bob. Bob receives the photon in the vertical/horizontal mode and records a horizontal photon. He used the correct mode but obtained the wrong measurement result and the wrong bit value. When Alice and Bob compare their sending and receiving modes they will end up with errors in the key (red data in the scorecards in the illustration). A NIST error-correction method will detect these errors, and Alice and Bob will know that Eve has been listening.



Mathematician Anastase Nakassis developed the error-correction method for NIST's quantum key distribution system.

wireless optical channel between two buildings 730 meters apart. A second system sends single photons through fiber.

Development of the testbed and measurement infrastructure, including new rules for managing quantum systems and data, draws on and integrates multiple disciplines. The testbed also provides a well-characterized environment for testing new photon sources and detectors and analyzing the performance of different sets of rules.

HIGH-SPEED QKD SYSTEM

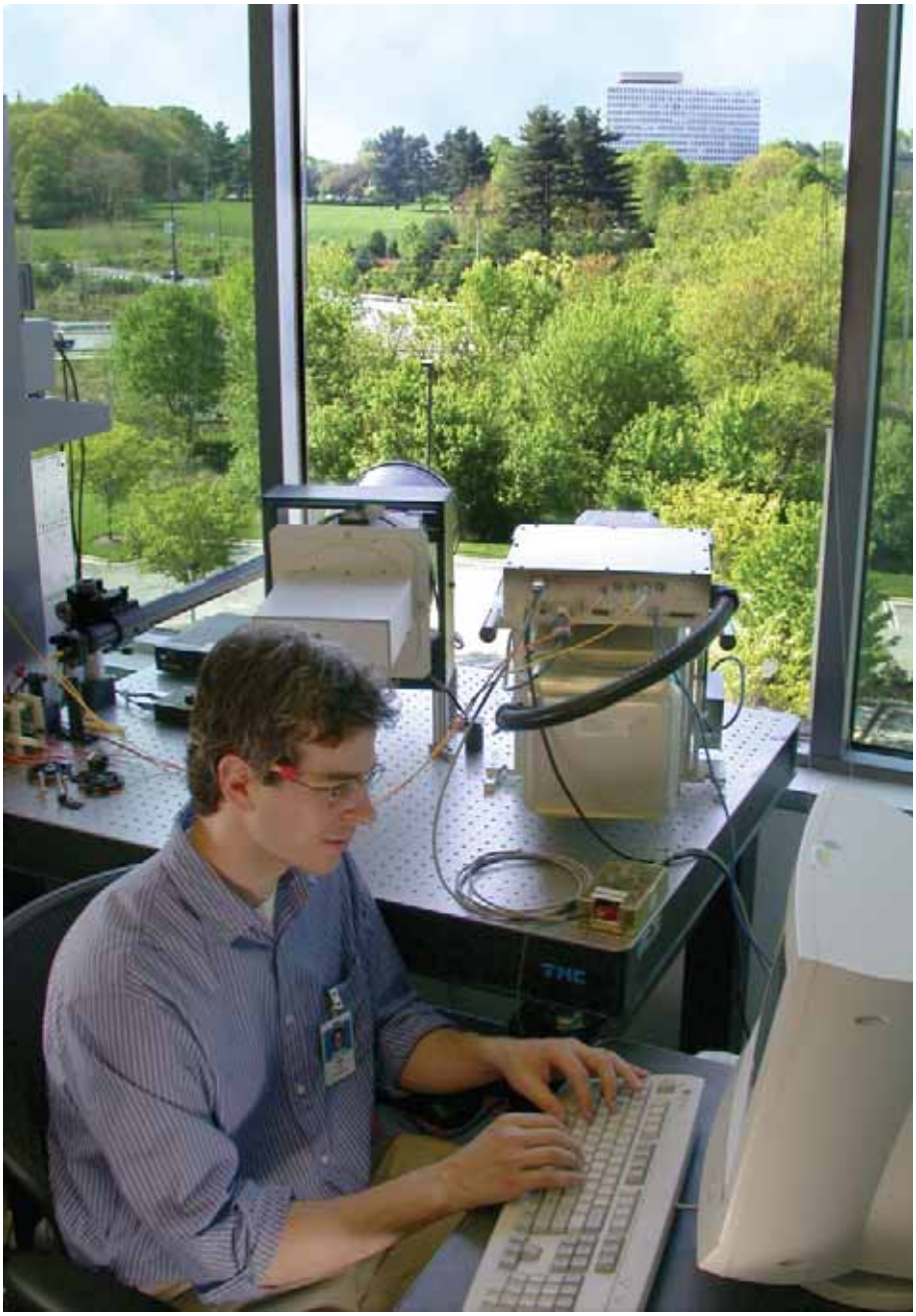
Using the testbed, NIST has built a QKD system that transmits a stream of individual photons to generate a verifiably secret key at a rate of 1 million bits per second. This rate is about 100 times faster than previously reported systems of this type. High speed is essential for QKD to become commercially viable and usable for a variety of applications, such as a recent NIST demonstration of streaming encrypted video. Previous systems produced keys at rates that would fill no more than one CD-ROM in 2 months; the NIST system could fill a CD-ROM in less than 2 hours.

QKD systems need to identify a photon from the sending laser amid many photons from other sources, such as the sun. To make this distinction, NIST scientists time-stamp the QKD photons, then look for them only when one is expected to arrive. They also select photons of a particular frequency, or color. NIST adapted techniques used in high-speed telecommunications to increase the rate at which the system can look for photons.

The received photons are processed at high speed, in real time, by circuit boards designed at NIST, so that keys are produced automatically. NIST computer scientists also developed a high-speed approach to error correction adapted from telecommunications techniques. This makes it possible to correct bit errors rapidly without time-consuming discussions between sender and receiver and without wasting a great deal of the key by revealing it to a potential eavesdropper.

SINGLE-PHOTON DETECTORS

Many photon detectors do not efficiently detect single photons, cannot distinguish between one or more photons arriving at the same time, and produce high false (or dark) count rates due to random "noise." They also tend to operate best with visible light instead of the near-infrared light needed for long-distance fiber-optic communications. NIST scientists have demonstrated single-photon detectors that operate with near-infrared light and count more than 100,000 photons per second while reducing false counts



to virtually zero. The detection efficiency—the proportion of received photons that are actually detected—exceeds 85 percent.

SINGLE-PHOTON SOURCES

Existing light sources, such as lasers, cannot produce single photons reliably. NIST is developing single-photon "turnstiles" that produce pulses of light containing exactly one photon. For instance, NIST has demonstrated efficient production of single photons from a "quantum dot," 10 to 20 nanometers wide, made of semiconductor materials. Another method uses a special crystal that converts one photon to a pair of photons with lower energies. Because the photons are created in pairs, the detection of one indicates, with absolute certainty, the existence of the other. One photon is intercepted by a detector and the other is used for communications or for evaluating and calibrating other single-photon sources or detectors. NIST is working to increase the precision and reliability so the technique can be broadly applied.

Physicist Joshua Bienfang sets up the NIST quantum key distribution system to receive a stream of photons from the top floor of another building (shown in the background).

Developing quantum computer architectures is like designing today's supercomputers in the era of vacuum tube computing, before the invention of transistors.

Emanuel Knill, NIST mathematician

QUANTUM INFORMATION THEORY

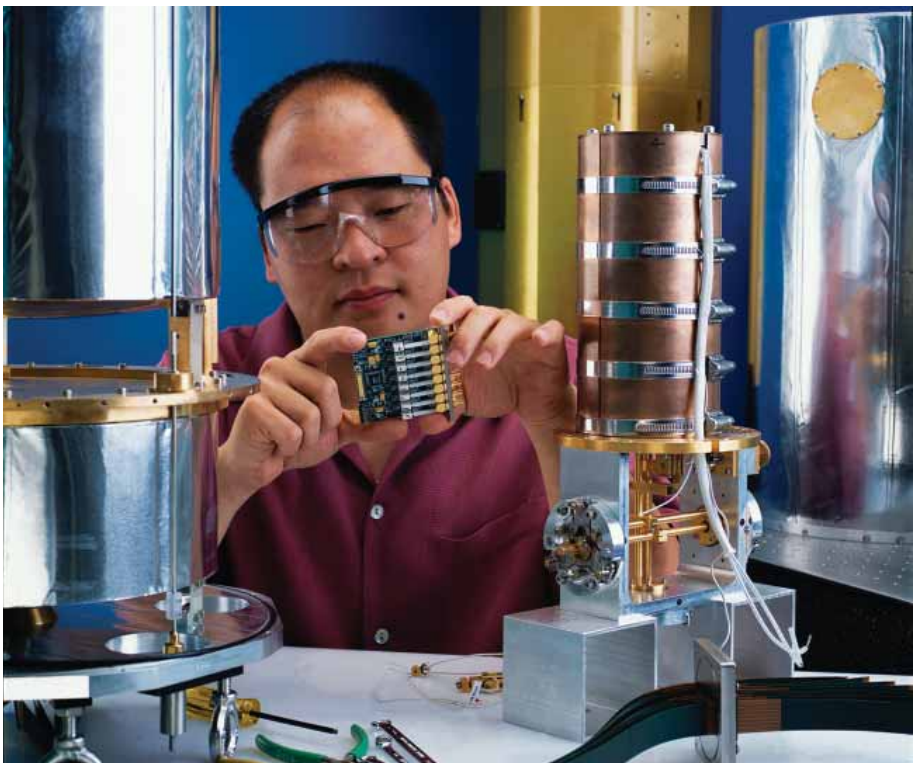
Quantum information provides a powerful new model for information processing, but its capabilities have yet to be fully understood and are also open to misinterpretation. To transform today's experimental components into reliable, well-engineered computers and communications systems, theoretical research is needed. In much the same manner that John von Neumann created the architecture still used to build classical computers—the four main parts are the processor, control unit, memory, and input/output devices—information theorists are beginning to create the paradigm for quantum systems.

Questions to be answered include: What fundamental operations are needed for the central processing unit? How should hundreds of logic operations be connected so they interact smoothly? What basic programming is needed for the central processing unit? How can efficient quantum circuits be created on the fly? What are the best error-correction techniques and how can they be efficiently implemented? How does one move information in a quantum computer without wires? What quantities can, or cannot, be computed more efficiently on a quantum computer than on a classical computer? And, what algorithms will translate the output (ordinary 1s and 0s) into meaningful results that reflect the inherent quantum parallel processing involved?

For quantum communications: Is quantum cryptography really "unbreakable"? Can it ever work fast and reliably enough, at sufficiently low cost, for widespread use?

NIST contributions to quantum information theory include:

- An error-correction architecture that could make quantum computers much easier to build than previously imagined. The NIST architecture would enable reliable computing even if individual logic operations made small errors as often as 3 percent of the time—performance levels already achieved at NIST with atomic-ion traps. The proposed architecture could tolerate error rates several hundred times larger than scientists had generally thought acceptable.
- A "communications bus" scheme allowing distant qubits in a quantum computer to communicate as if they were in direct contact. Imagine a transit bus that instantly transports commuters to their destination. Rather than passing data through a long line of qubits in between, the NIST scheme would create a chain of entangled pairs of empty "bus qubits" between two distant memory qubits that need to exchange information. Then the ends of the chain would be entangled with each other. This entanglement can be used to perform joint operations on qubits near opposite endpoints, in ways that increase processing speed and reduce errors.
- An analysis of security vulnerabilities suggesting that some implementations of quantum cryptography are not really "unbreakable." The analysis shows that some eavesdropping approaches could break an encryption scheme that relies on manipulation and return of entangled qubits to create a shared "key." This suggests that, at least in some cases, quantum cryptography can be vulnerable to attacks not envisioned by system designers. The history of cryptography is full of examples of approaches that were believed to be secure but shown to be vulnerable to novel attacks, often years after their design.



Physicist Sae Woo Nam has developed single-photon detectors with record efficiency at telecommunications wavelengths.

Selected NIST Publications

QUANTUM COMPUTING

E. Knill. Quantum computing with very noisy devices. *Nature* 434:39–44 (2005)

R. McDermott, R.W. Simmonds, M. Steffen, K.B. Cooper, K. Cicak, K. Osborn, S. Oh, D.P. Pappas, and J.M. Martinis. Simultaneous state measurement of coupled Josephson phase qubits. *Science* 307:1299–1302 (2005)

J. Chiaverini, D. Leibfried, T. Schaetz, M.D. Barrett, R.B. Blakestad, J. Britton, W.M. Itano, J.D. Jost, E. Knill, C. Langer, R. Ozeri, and D.J. Wineland. Realization of quantum error correction. *Nature* 432:602–605 (2004)

B. Laburthe-Tolra, K.M. O'Hara, J.H. Huckans, W.D. Phillips, S.L. Rolston, and J.V. Porto. Observation of reduced three-body recombination in a correlated 1D degenerate Bose gas. *Physical Review Letters* 92, 190401 (2004)

M.D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W.M. Itano, J.D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, and D.J. Wineland. Deterministic quantum teleportation of atomic qubits. *Nature* 429:737–739 (2004)

J.V. Porto, S. Rolston, B. Laburthe-Tolra, C.J. Williams, and W.D. Phillips. Quantum information with neutral atoms as qubits. *Philosophical Transactions of the Royal Society London Series A 361*, 1417–1427 (2003)

D. Kielpinski, C. Monroe, and D.J. Wineland. Architecture for a large-scale ion-trap quantum computer. *Nature* 417:709–711 (2002)

QUANTUM COMMUNICATIONS

A. Nakassis, J. Bienfang, and C. Williams. Expeditious reconciliation for practical quantum key distribution. *Quantum Information and Computation II, Proc. SPIE* Vol. 5436 (2004)

M. Ware and A. Migdall. Single photon detector characterization using correlated photons: the march from feasibility to metrology. *Journal of Modern Optics* 51 (9-10):1549–1557 (2004)

J.C. Bienfang, A.J. Gross, A. Mink, B.J. Hershman, A. Nakassis, X. Tang, R. Lu, D.H. Su, C.W. Clark, C.J. Williams, E.W. Hagley, and J. Wen. Quantum key distribution with 1.25 Gbps clock synchronization. *Optics Express* 12(9):2011–2016 (2004)

A.J. Miller, S.W. Nam, J.M. Martinis, and A.V. Sergienko. Demonstration of a low-noise near-infrared photon counter with multi-photon discrimination. *Applied Physics Letters* 83(4):791–793 (2003)

Photo & Illustration Credits

Pages 2, 9 (top), 11 (top), 15 © Geoffrey Wheeler

Pages 3-4, Kelly Talbott/NIST

Page 6 (left), 11 (bottom), 13, back pocket, © Robert Rathe

Page 6 (right), NIST

Page 7, M.D. Barrett and J. Jost/NIST

Page 9 (bottom), Raymond Simmonds/NIST

Page 12, © Loel Barr

Page 14, Gail Porter/NIST

NIST Special Publication 1042

Editors: Laura Ost and Carl Williams

Graphic Design: Ion Design

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Michelle O'Neill, Acting Under Secretary for Technology

National Institute of Standards and Technology
William A. Jeffrey, Director

August 2005

DIE LINE - DO NOT PRINT!

NIST QUANTUM INFORMATION PROGRAM

The Quantum Information Program is an interdisciplinary, collaborative effort of the NIST Physics Laboratory, Electronics and Electrical Engineering Laboratory, and Information Technology Laboratory.

Coordinator: Carl Williams
carl.williams@nist.gov, (301) 975-3531

For further information visit:
http://qubit.nist.gov
http://math.nist.gov/quantum/
http://www.nist.gov

Carl Williams is chief of the NIST Atomic Physics Division and coordinator of the Quantum Information Program.

NIST Quantum Information Program
100 Bureau Drive, Stop 8420
Gaithersburg, MD 20899-8420

http://qubit.nist.gov